RISK is an acronym…

Research: Study and understand the ever-changing risk environment; it all starts here.

Investigations: Uncover the who, what, when, how, and why behind security incidents.

Solutions: Leverage lessons from "R" and "I" for innovation and product improvement.

Knowledge: Distribute valuable research to Verizon and the security community.

…but also a philosophy

To properly manage risk, we must measure it. To properly measure risk, we must understand our information *assets*, the *threats* that can harm them, the *impact* of such events, and the *controls* that offer protection.

This is the purpose of intelligence - to measure each landscape to improve risk management capability

RISK Intelligence mission and scope of operations

"Our primary objective is to improve information security operations and decision-making through actionable intelligence and credible research."

Tactical Intel

Goal: Improve network threat **detection** and incident response capabilities

- Track indicators of compromise
  - Collect, enrich, distribute
- Track threat actor groups
  - Region, motive, TTPs, victims, etc.
- Track criminal & espionage campaigns
- Support integration of intelligence into Verizon products

"Detections"

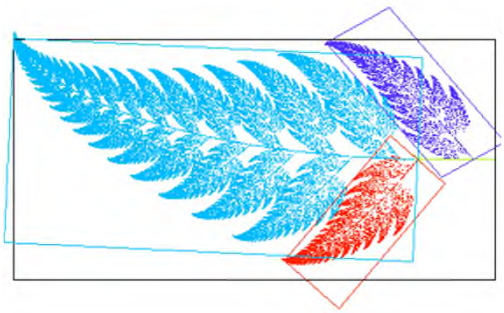
Strategic Intel

Goal: Improve infosec management by supporting informed **decision** making

- Collect data relevant to infosec management and decision making
- Conduct analysis to decrease uncertainty & increase manageability
- Publish credible research addressing key challenges to the infosec industry
- Foster information sharing & research within the infosec community

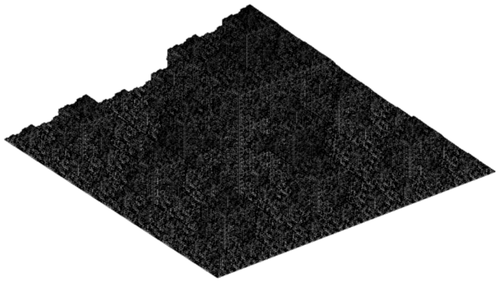
"Decisions"

Setting the Stage: Patterns

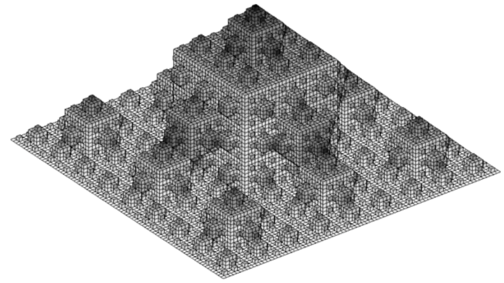


"Nature uses a few simple, self-similar, and repeating patterns-- fractals --to build energy and atoms into the familiar forms of everything from roots, rivers, and trees, to rocks, mountains, and us."

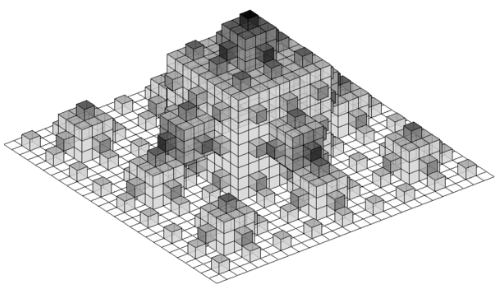
- Gregg Braden, *Fractal Time, The Secret of 2012 and a New World Age*



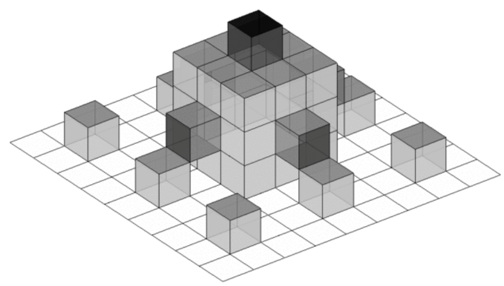
Description: Animation of quadratic Koch 3D (Recusion levels: 1 to 5). Author: Guillaume Jacquenot



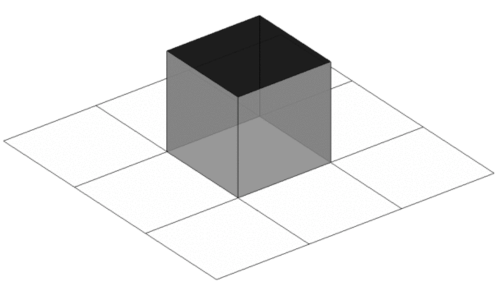
Description: Animation of quadratic Koch 3D (Recusion levels: 1 to 5). Author: Guillaume Jacquenot



Description: Animation of quadratic Koch 3D (Recusion levels: 1 to 5). Author: Guillaume Jacquenot



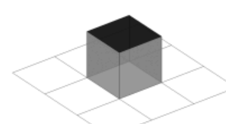
Description: Animation of quadratic Koch 3D (Recusion levels: 1 to 5). Author: Guillaume Jacquenot



Description: Animation of quadratic Koch 3D (Recusion levels: 1 to 5). Author: Guillaume Jacquenot

Threats to your data:

<or>



???

Data Breach Investigations Report (DBIR)

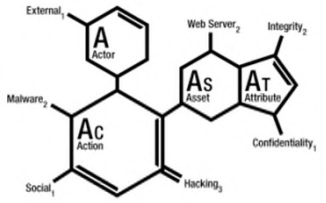
An ongoing study that analyzes forensic evidence to uncover how sensitive data is stolen from organizations, who's doing it, why they're doing it, and what might be done to prevent it.

AFP · CERT · Software Engineering Institute Carnegie Mellon · Consortium for Cybersecurity Action · CyberSecurity Malaysia · Deloitte. · EC3 · ES ISAC Electricity Sector Information Sharing Analysis Center · Danish Defence Intelligence Service · FE · GC Partners · Guardia Civil · Homeland Security · IRISS · Politi · Politie · ThreatSim™

The Main Act: 2013 DBIR Findings

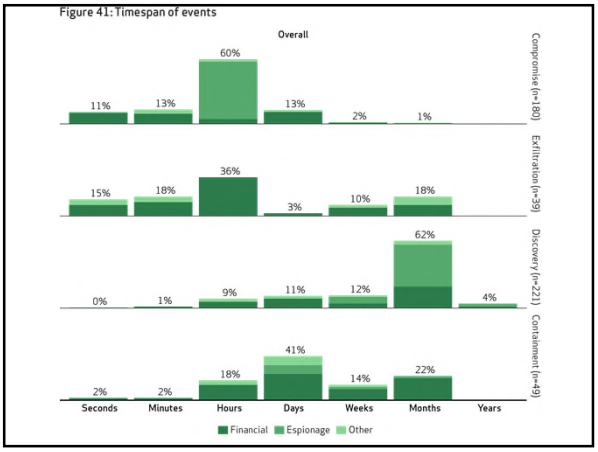
verizon

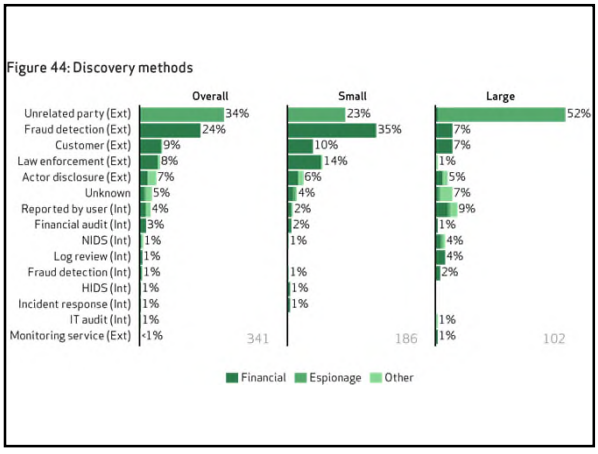
Vocabulary for
Event
Recording and
Incident
Sharing

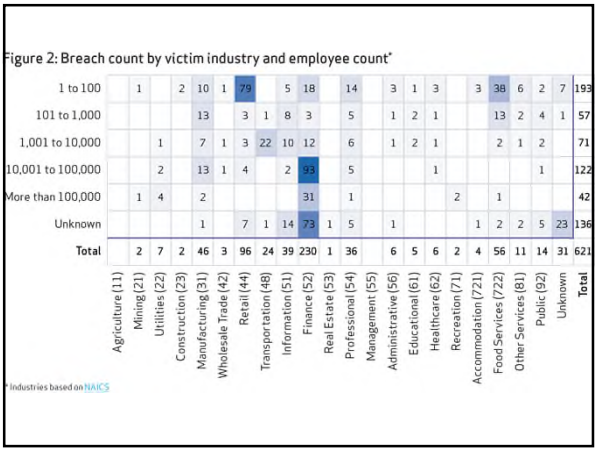


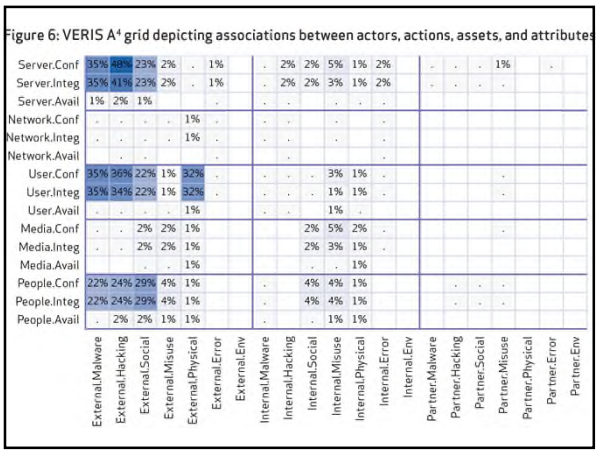
provides a common language for describing security incidents in a structured and repeatable manner

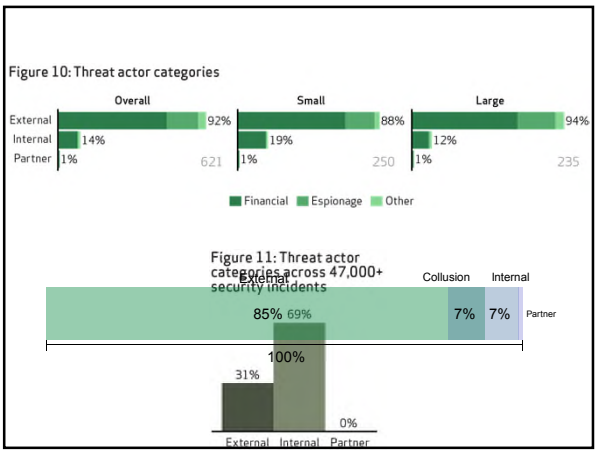
http://veriscommunity.net

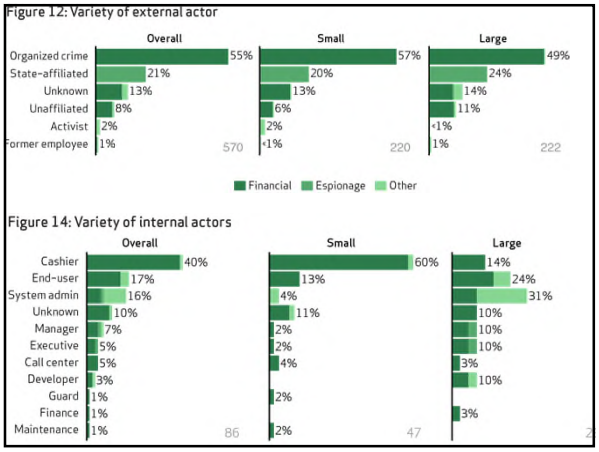


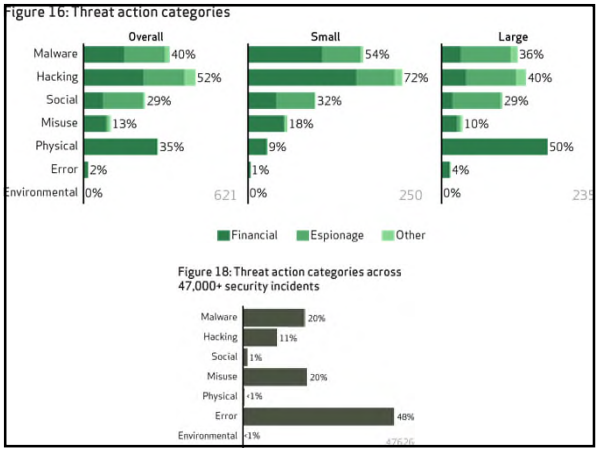




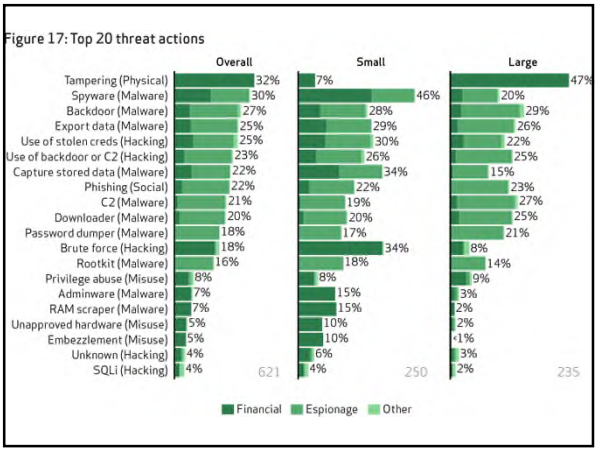


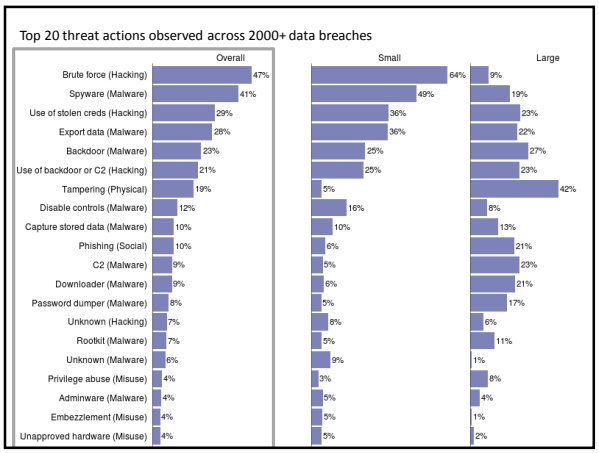


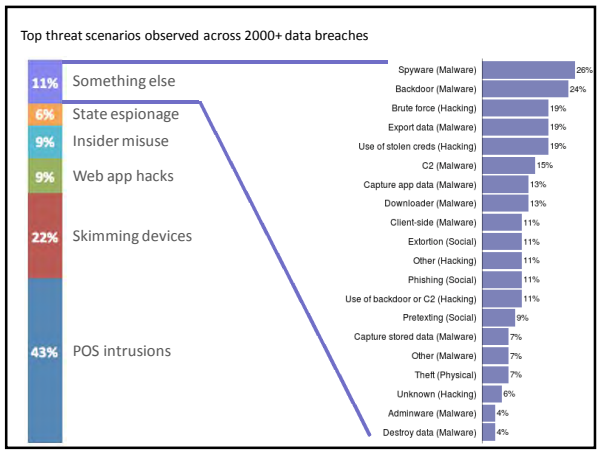


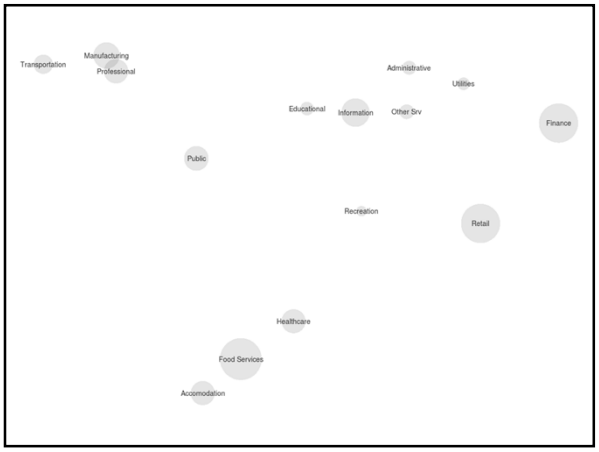


Adware , Backdoor , Brute force , Capture app data , Capture stored data , Client-side , C2 , Destroy data , Disable controls , DoS , Downloader , Exploit vuln , Export data , Packet sniffer , Password dumper , Ram scraper , Ransomware , Rootkit , Scan network , Spam , Spyware , SQL injection , Utility , Worm , Abuse of functionality , Brute force , Buffer overflow , Cache poisoning , Credential/session prediction , Cross-site request forgery , Cross-site scripting , Cryptanalysis , Denial of service , Footprinting and fingerprinting , Forced browsing , Format string attack , Fuzz testing , HTTP request smuggling , HTTP request splitting , HTTP response smuggling , HTTP Response Splitting , Integer overflows , LDAP injection , Mail command injection , Man-in-the-middle attack , Null byte injection , Offline cracking , OS commanding , Path traversal , Remote file inclusion , Reverse engineering , Routing detour , Session fixation , Session replay , Soap array abuse , Spoofing element , SQL injection , SSL injection , URL redirector abuse , Use of backdoor or C2 , Use of stolen creds , XML attribute blowup , XML entity expansion , XML external entities , XML injection , XPath injection , XQuery injection , Baiting , Bribery , Elicitation , Extortion , Forgery , Influence , Scam , Phishing , Pretexting , Propaganda , Spam , Knowledge abuse , Privilege abuse , Embezzlement , Data mishandling , Email misuse , Net misuse , Illicit content , Unapproved workaround , Unapproved hardware , Unapproved software , Assault , Sabotage , Snooping , Surveillance , Tampering , Theft , Wiretapping , Classification error , Data entry error , Disposal error , Gaffe , Loss , Maintenance error , Misconfiguration , Misdelivery , Misinformation , Omission , Physical accidents , Capacity shortage , Programming error , Publishing error , Malfunction , Deterioration , Earthquake , EMI , ESD , Temperature , Fire , Flood , Hazmat , Humidity , Hurricane , Ice , Landslide , Lightning , Meteorite , Particulates , Pathogen , Power failure , Tornado , Tsunami , Vermin , Volcano , Leak , Wind




Top 20 threat actions observed across 2000+ data breaches
Overall
Small
Large
Brute force (Hacking) 47% 64% 9%
Spyware (Malware) 41% 49% 19%
Use of stolen creds (Hacking) 29% 36% 23%
Export data (Malware) 28% 36% 22%
Backdoor (Malware) 23% 25% 27%
Use of backdoor or C2 (Hacking) 21% 25% 23%
Tampering (Physical) 19% 5% 42%
Disable controls (Malware) 12% 16% 8%
Capture stored data (Malware) 10% 10% 13%
Phishing (Social) 10% 6% 21%
C2 (Malware) 9% 5% 23%
Downloader (Malware) 9% 6% 21%
Password dumper (Malware) 8% 5% 17%
Unknown (Hacking) 7% 8% 6%
Rootkit (Malware) 7% 5% 11%
Unknown (Malware) 6% 9% 1%
Privilege abuse (Misuse) 4% 3% 8%
Adminware (Malware) 4% 5% 4%
Embezzlement (Misuse) 4% 5% 1%
Unapproved hardware (Misuse) 4% 5% 2%


Top threat scenarios observed across 2000+ data breaches
11% Something else
6% State espionage
9% Insider misuse
9% Web app hacks
22% Skimming devices
43% POS intrusions
Spyware (Malware) 26%
Backdoor (Malware) 24%
Brute force (Hacking) 19%
Export data (Malware) 19%
Use of stolen creds (Hacking) 19%
C2 (Malware) 15%
Capture app data (Malware) 13%
Downloader (Malware) 13%
Client-side (Malware) 11%
Extortion (Social) 11%
Other (Hacking) 11%
Phishing (Social) 11%
Use of backdoor or C2 (Hacking) 11%
Pretexting (Social) 9%
Capture stored data (Malware) 7%
Other (Malware) 7%
Theft (Physical) 7%
Unknown (Hacking) 6%
Adminware (Malware) 4%
Destroy data (Malware) 4%


Transportation
Manufacturing
Professional
Administrative
Utilities
Educational
Information
Other Srv
Finance
Public
Recreation
Retail
Healthcare
Food Services
Accomodation

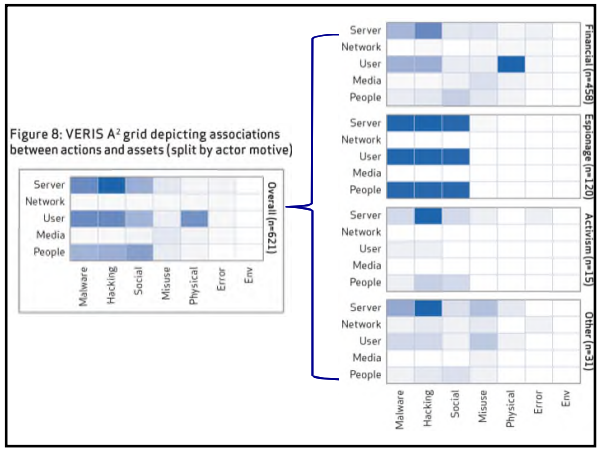


Figure 8: VERIS A² grid depicting associations between actions and assets (split by actor motive)
Server
Network
User
Media
People
Overall (n=621)
Financial (n=558)
Espionage (n=120)
Activism (n=15)
Other (n=31)
Malware
Hacking
Social
Misuse
Physical
Error
Env

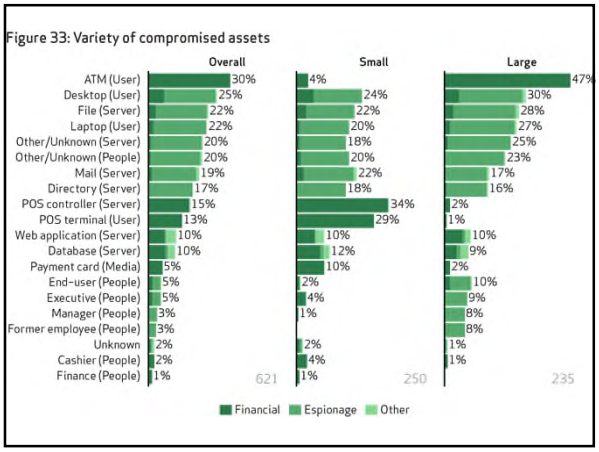


Figure 33: Variety of compromised assets
Overall
Small
Large
ATM (User) 30% 4% 47%
Desktop (User) 25% 24% 30%
File (Server) 22% 22% 28%
Laptop (User) 22% 20% 27%
Other/Unknown (Server) 20% 18% 25%
Other/Unknown (People) 20% 20% 23%
Mail (Server) 19% 22% 17%
Directory (Server) 17% 18% 16%
POS controller (Server) 15% 34% 2%
POS terminal (User) 13% 29% 1%
Web application (Server) 10% 10% 10%
Database (Server) 10% 12% 9%
Payment card (Media) 5% 10% 2%
End-user (People) 5% 2% 10%
Executive (People) 5% 4% 9%
Manager (People) 3% 1% 8%
Former employee (People) 3% 8%
Unknown 2% 2% 1%
Cashier (People) 2% 4% 1%
Finance (People) 1% 1%
621
250
235
Financial
Espionage
Other

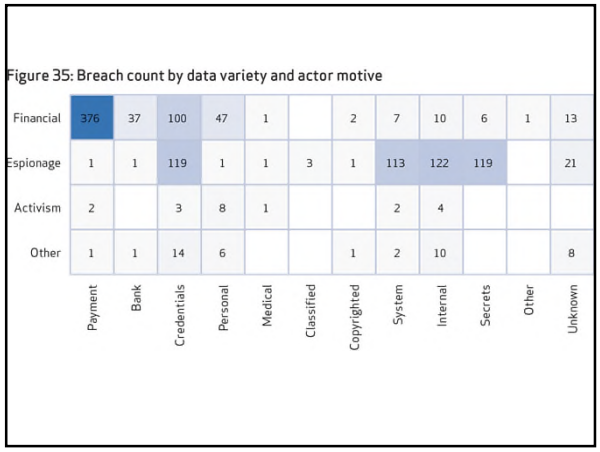
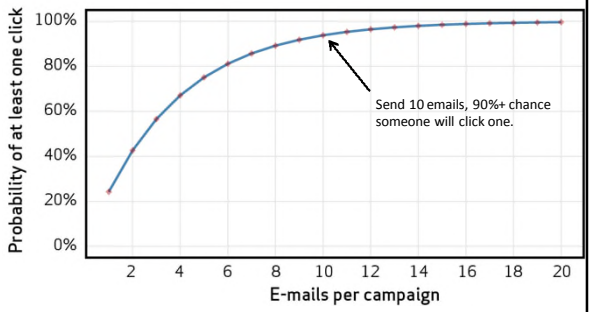


Figure 35: Breach count by data variety and actor motive
Financial 376 37 100 47 1 2 7 10 6 1 13
Espionage 1 1 119 1 1 3 1 113 122 119 21
Activism 2 3 8 1 2 4
Other 1 1 14 6 1 2 10 8
Payment
Bank
Credentials
Personal
Medical
Classified
Copyrighted
System
Internal
Secrets
Other
Unknown

Table 1: Profiling threat actors

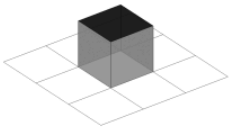
	ORGANIZED CRIME	STATE-AFFILIATED	ACTIVISTS
VICTIM INDUSTRY	Finance Retail Food	Manufacturing Professional Transportation	Information Public Other Services
REGION OF OPERATION	Eastern Europe North America	East Asia (China)	Western Europe North America
COMMON ACTIONS	Tampering (Physical) Brute force (Hacking) Spyware (Malware) Capture stored data (Malware) Adminware (Malware) RAM Scraper (Malware)	Backdoor (Malware) Phishing (Social) Command/Control (C2) (Malware, Hacking) Export data (Malware) Password dumper (Malware) Downloader (Malware) Stolen creds (Hacking)	SQLi (Hacking) Stolen creds (Hacking) Brute force (Hacking) RFI (Hacking) Backdoor (Malware)
TARGETED ASSETS	ATM POS controller POS terminal Database Desktop	Laptop/desktop File server Mail server Directory server	Web application Database Mail server
DESIRED DATA	Payment cards Credentials Bank account info	Credentials Internal organization data Trade secrets System info	Personal info Credentials Internal organization data

Figure 28: The inevitability of the click



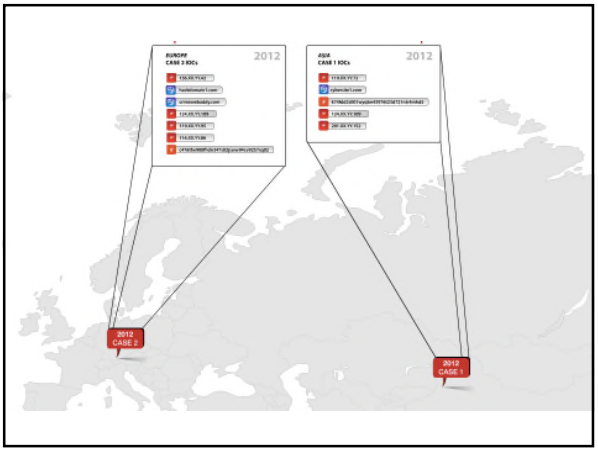
Threats to your data:

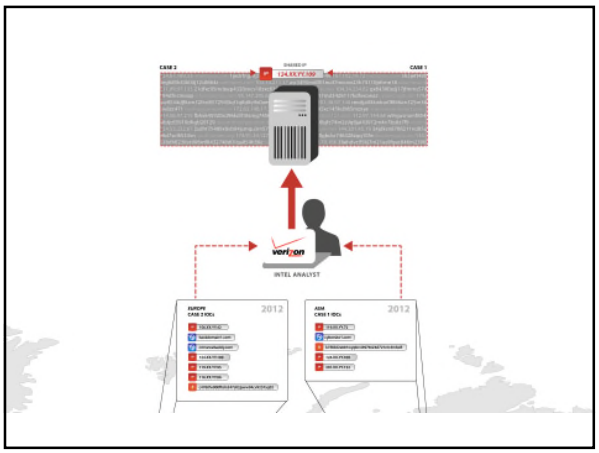
<or>

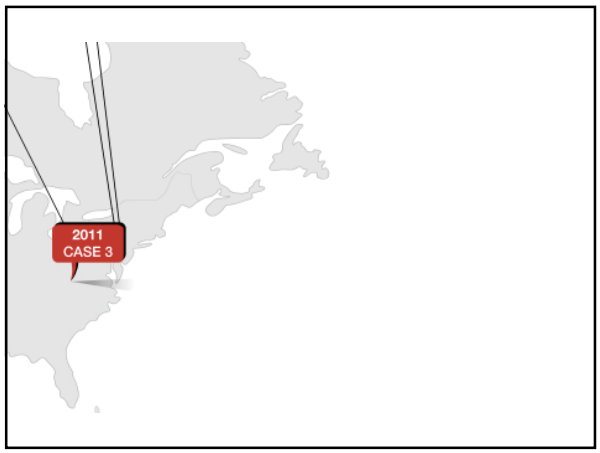


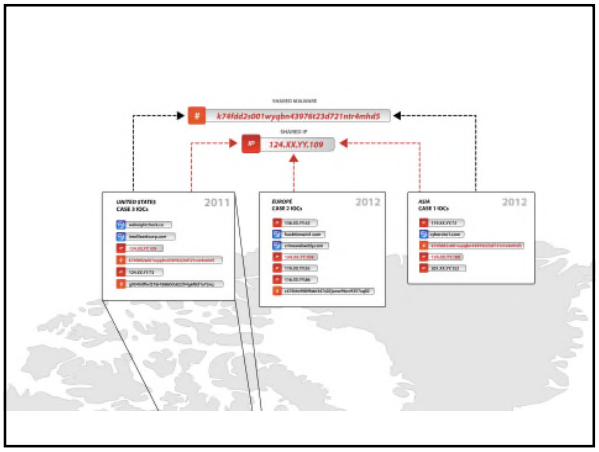
???

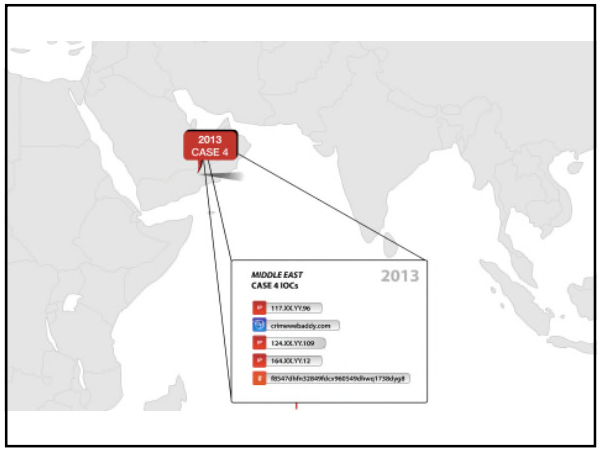
So What? #1

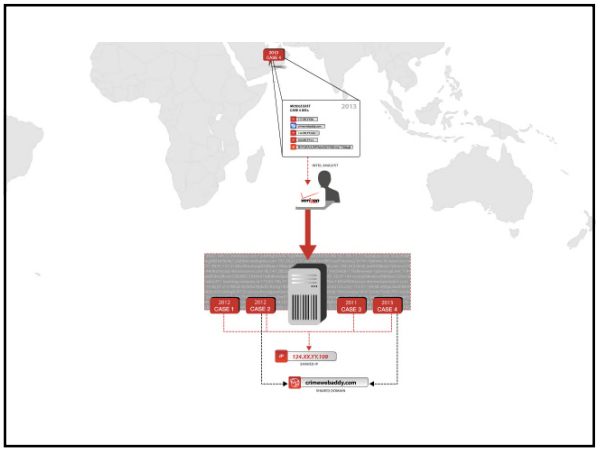


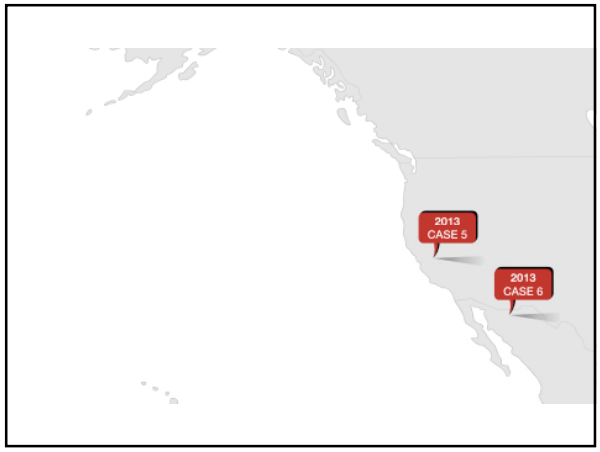

verizon
INTEL ANALYST
2012
2012

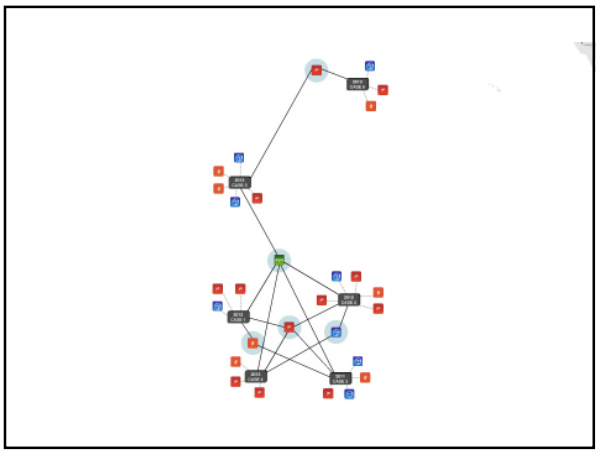

2011
CASE 3


124.XX.YY.109
2011
2012
2012


2013
CASE 4
MIDDLE EAST
CASE 4 IOCs
2013

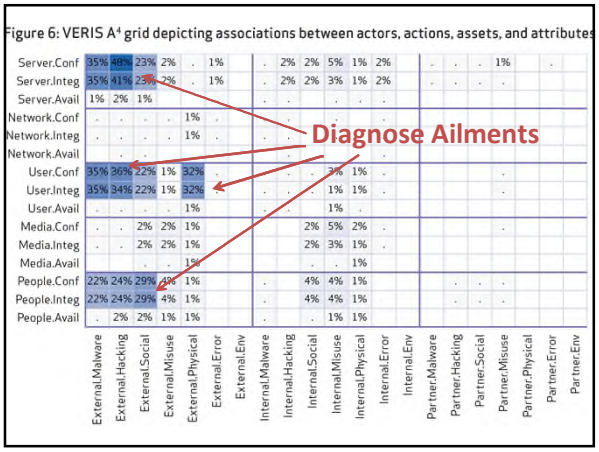

2013
verizon
crimewebaddy.com

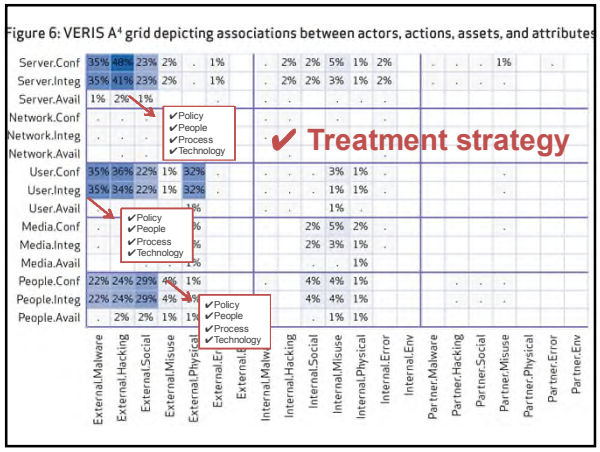

2013
CASE 5
2013
CASE 6

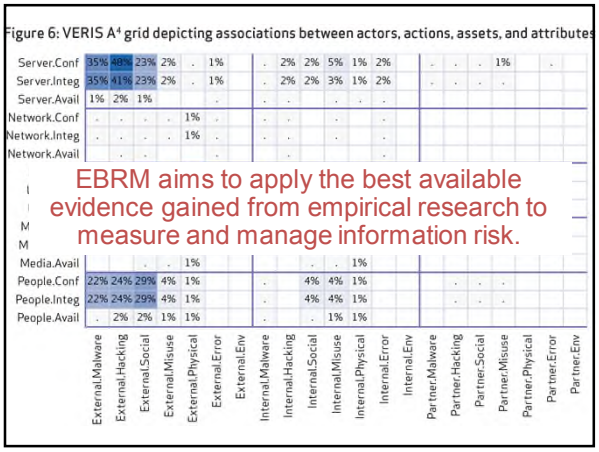


So What? #2

verizon







Recommendations

- Eliminate unnecessary data; keep tabs on what's left.
- Ensure essential controls are met; regularly check that they remain so.
- Collect, analyze and share incident data to create a rich data source that can drive security program effectiveness.
- Collect, analyze, and share tactical threat intelligence, especially Indicators of Compromise (IOCs), that can greatly aid defense and detection.
- Without deemphasizing prevention, focus on better and faster detection through a blend of people, processes, and technology.
- Regularly measure things like "number of compromised systems" and "mean time to detection" in networks. Use them to drive security practices.
- Evaluate the threat landscape to prioritize a treatment strategy. Don't buy into a "one-size fits all" approach to security.
- If you're a target of espionage, don't underestimate the tenacity of your adversary. Nor should you underestimate the intelligence and tools at your disposal.

Additional Information

- Download DBIR – www.verizonenterprise.com/dbir
- Learn about VERIS - www.veriscommunity.net
- Ask a question – DBIR@verizon.com
- Read our blog - http://www.verizonenterprise.com/security/blog/
- Follow on Twitter - @vzdbir and hashtag #dbir